

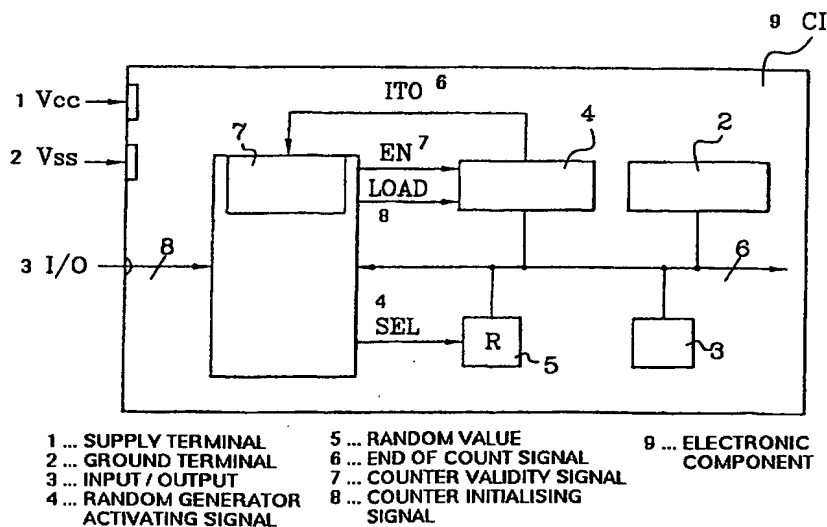


DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : G06F 1/00	A1	(11) Numéro de publication internationale: WO 00/23866 (43) Date de publication internationale: 27 avril 2000 (27.04.00)
(21) Numéro de la demande internationale: PCT/FR99/02521 (22) Date de dépôt international: 15 octobre 1999 (15.10.99) (30) Données relatives à la priorité: 98/12988 16 octobre 1998 (16.10.98) FR (71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gemenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): ANGUIA, Philippe [FR/FR]; 227, chemin de Riquet, F-13400 Aubagne (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).		(81) Etats désignés: AU, BR, CA, CN, IN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Avec rapport de recherche internationale.</i>

(54) Title: ELECTRONIC COMPONENT FOR MASKING EXECUTION OF INSTRUCTIONS OR DATA MANIPULATION

(54) Titre: COMPOSANT ELECTRONIQUE ET PROCEDE POUR MASQUER L'EXECUTION D'INSTRUCTIONS OU LA MANIPULATION DE DONNEES



(57) Abstract

The invention concerns an electronic component (CI) comprising a microprocessor (1) and storage means (2, 3) for executing a main programme. A random value (R) counter (4) generates in output an end of count signal (ITO) to suspend execution of the main programme while a secondary programme is being executed. The invention is applicable to smart cards.

(57) Abrégé

Un composant électronique (CI) comprend un microprocesseur (1) et des moyens de mémorisation (2, 3) pour exécuter un programme principal. Un compteur (4) d'une valeur aléatoire (R) génère en sortie un signal d'information de fin de comptage (ITO) pour suspendre l'exécution du programme principal le temps de l'exécution d'un programme secondaire. Application aux cartes à puces.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**COMPOSANT ÉLECTRONIQUE ET PROCÉDÉ POUR MASQUER
L'EXÉCUTION D'INSTRUCTIONS OU LA MANIPULATION DE
DONNÉES**

La présente invention concerne un composant électronique et un procédé pour masquer l'exécution d'instructions ou la manipulation de données.

La présente invention concerne plus particulièrement les composants électroniques utilisés dans des applications où l'accès à des services ou à des données est sévèrement contrôlé. De tels composants ont une architecture formée autour d'un microprocesseur et de mémoires. Ils mettent en oeuvre des algorithmes utilisant des données secrètes contenues dans le composant, inaccessibles de l'extérieur. Une donnée secrète peut ainsi servir à valider une transaction électronique telle qu'un achat, sans que cette donnée soit à aucun moment accessible de l'extérieur du composant.

Cependant, l'observation de certains paramètres extérieurs tels que les données échangées avec un système extérieur, ou le courant consommé sur la borne d'alimentation du composant, permet dans certains cas de retrouver des informations concernant le composant, au moyen de traitements statistiques. En particulier, à partir de l'observation en fonction du temps des informations circulant sur le bus de données, en général un bus série, il est possible de faire une corrélation entre ces informations et le déroulement de l'algorithme mis en oeuvre dans le composant.

Il peut être également possible de faire une corrélation de ces informations avec l'observation de la consommation de courant en fonction du temps. Il est alors possible de déduire la valeur d'un bit manipulé

dans une instruction. On sait en effet qu'à un instant donné, la consommation en courant d'une instruction particulière varie selon la valeur "0" ou "1" du bit manipulé.

5 La présente invention a pour but de masquer l'exécution d'instructions ou la manipulation de données dans le composant, afin de rendre stérile l'observation de paramètres externes du composant électronique.

10 Selon l'invention, on prévoit d'interrompre de manière aléatoire l'exécution du programme principal mis en oeuvre par le composant électronique, pour exécuter un programme secondaire. De cette manière, le déroulement du programme change tout le temps. Vu de
15 l'extérieur, il n'est plus possible de faire des traitements statistiques, car les courbes relevées sont toutes décalées temporellement, de manière aléatoire. Si on prend l'exemple de l'observation des données échangées, les temps de réponse de la carte à n'importe
20 quelle commande extérieure changent tout le temps, en sorte qu'il n'est plus possible d'en déduire une quelconque information pertinente.

En ce qui concerne l'observation de la consommation en courant, cette consommation en courant en fonction
25 du temps est elle même découpée, diffusée par rapport à la courbe de consommation normale, en sorte que l'on ne peut obtenir aucune information pertinente.

Ainsi, telle que caractérisée, l'invention concerne un composant électronique comprenant au moins un
30 microprocesseur et des moyens de mémorisation pour exécuter un programme principal.

Selon l'invention, le composant comprend en outre un compteur d'une valeur aléatoire générant en sortie
une information pour suspendre l'exécution dudit
35 programme le temps de l'exécution d'un programme secondaire.

Dans un mode de réalisation de l'invention, ce temps d'exécution du programme secondaire est constant. Dans un autre mode de réalisation de l'invention, ce temps d'exécution est variable. Il peut même être aléatoire.

Dans un perfectionnement, on prévoit que ce programme secondaire active des moyens de consommation en courant, qui vont venir fausser la courbe de consommation en courant du composant, rendant le masquage des opérations exécutées et des données manipulées encore plus efficace.

L'invention concerne aussi un procédé de masquage de l'exécution d'instruction ou de la manipulation de données dans un composant électronique.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- la figure 1 représente un schéma-bloc d'un composant électronique selon l'invention; et

- la figure 2 représente une variante du schéma-bloc d'un composant électronique selon une variante de l'invention.

La figure 1 représente un schéma-bloc simplifié d'un composant électronique CI selon l'invention. Il comprend un microprocesseur 1 et des ressources internes qui sont connectés à un bus de données 6. Les ressources internes comprennent notamment des mémoires, dans l'exemple, une mémoire programme 2 et une mémoire de travail 3, un compteur 4 et un générateur 5 d'une valeur aléatoire R.

Le composant électronique CI comprend différentes bornes de connexion externe. Dans l'exemple, c'est un composant à entrée/sortie série de données, avec donc une borne I/O d'entrée/sortie de données. Il comprend aussi une borne de masse VSS, une borne d'alimentation

VCC et des bornes relatives à des signaux de contrôle (non représentés).

Le microprocesseur reçoit des instructions et des données sur un port d'entrée/sortie série 8, connecté à la borne d'entrée/sortie de données en relation avec un système externe.

Le microprocesseur génère en interne différents signaux de contrôle pour gérer les différentes ressources internes.

Parmi ces signaux de contrôle, on a représenté un signal de validation EN du compteur 4, un signal LOAD d'initialisation du compteur et un signal d'activation SEL du générateur aléatoire 5.

Quand il est validé (EN activé), le compteur génère un signal de fin de comptage IT0. Ce signal d'information de fin de comptage est utilisé comme signal d'interruption du microprocesseur. Il est ainsi connecté sur une entrée du port d'interruption 7 du microprocesseur. On notera que l'expression fin de comptage est une expression générale qui veut dire aussi bien que le compteur a fini de compter jusqu'à une valeur déterminée ou que le compteur a fini de décompter à zéro depuis une valeur déterminée.

On notera que dans l'exemple plus particulièrement représenté le compteur est une ressource matérielle.

Le microprocesseur 1 exécute un programme principal contenu en mémoire programme, relativement à des données ou des instructions reçues du port d'entrée sortie série 8, en relation avec un système externe.

Selon l'invention, l'exécution du programme principal est suspendue à des moments aléatoires, le temps de l'exécution d'un programme secondaire, contenu en mémoire programme.

Pour cela, au début du programme principal, on prévoit une routine d'initialisation du compteur avec une nouvelle valeur aléatoire. En pratique, cette

routine comprend des instructions pour invalider le compteur (EN désactivé), tirer une valeur aléatoire R dans le générateur aléatoire 5, charger (LOAD) cette valeur dans le compteur, puis activer le compteur (EN activé).

Lorsque le compteur a décompté jusqu'à zéro, il active le signal d'information de fin de comptage IT0, ce qui provoque une interruption sur le microprocesseur. L'exécution du programme principal est suspendu le temps de l'exécution (par le microprocesseur) du programme secondaire, correspondant à la routine de gestion de l'interruption considérée.

Le programme secondaire comprend au minimum la séquence déjà vue d'initialisation du compteur, à une nouvelle valeur aléatoire, pour qu'une nouvelle interruption puisse avoir lieu.

Ce programme secondaire peut correspondre à un nombre fixe d'instructions, auquel cas il s'exécute en temps constant. Par exemple, si le programme secondaire comprend seulement les instructions correspondant au tirage d'une nouvelle valeur aléatoire R dans le générateur 5 et au chargement du compteur 4 à cette nouvelle valeur R (initialisation), on a un programme secondaire exécutable en temps constant.

Dans ce cas, en plus de l'exécution du programme principal, on a des bouts de code (correspondant au programme secondaire) exécutés en temps constant à des moments aléatoires.

Dans une variante de l'invention, on prévoit que la durée d'exécution du programme secondaire soit variable.

Dans un premier exemple pratique de réalisation, le programme secondaire prévoit un test sur une donnée binaire, modifiée à chaque passage dans le programme, le nombre d'instructions exécutées ensuite étant fonction du résultat du test. On peut aussi prévoir que

la durée variable d'exécution dépende d'une fonction mathématique. Par exemple, si cette fonction mathématique nécessite un certain nombre de tours de calcul pour arriver au résultat, ce nombre de tours étant fonction des données d'entrée, on aura une durée d'exécution variable, dépendant d'une fonction mathématique. Toutes ces techniques pour arriver à une durée variable sont bien connues.

Dans un autre exemple pratique, on prévoit que cette durée d'exécution variable soit aléatoire. On prévoit dans cet exemple que le programme secondaire comprend la désactivation du compteur, le tirage d'une nouvelle valeur aléatoire, le décomptage jusqu'à zéro de cette valeur dans une boucle de décomptage, puis l'initialisation du compteur à une nouvelle valeur aléatoire.

Dans cette variante, on introduit dans l'exécution du programme principal, des bouts de code exécutés en temps aléatoire à des moments aléatoires.

En pratique, de nombreuses variantes de l'invention sont possibles.

Notamment, pour ne pas trop dégrader le temps d'exécution du programme principal, on peut prévoir de limiter dans le temps la durée totale des retards dus à l'exécution du ou des programmes secondaires.

Dans un autre mode de réalisation de l'invention, on prévoit non seulement de suspendre l'exécution du programme principal à des moments aléatoires, mais aussi de prévoir une consommation en courant supplémentaire, qui va brouiller la consommation en courant due à l'exécution du programme principal.

Cette consommation en courant supplémentaire peut être due, de façon instantanée, à des instructions prévues dans le programme secondaire. Par exemple, on peut prévoir dans ce programme secondaire, d'exécuter

des tours de calcul d'un algorithme, par exemple d'un algorithme de cryptographie.

A cette exécution va correspondre une consommation en courant instantanée, c'est à dire le temps de l'exécution de l'instruction, qui va brouiller la consommation normale du programme principal en venant s'intercaler dans la consommation de courant normale en fonction du temps due à l'exécution du programme principal.

On peut aussi prévoir que cette consommation de courant supplémentaire ait un effet durable pendant un certain temps. Le programme secondaire prévoit alors d'activer des moyens de consommation de courant, qui vont consommer du courant au moins un certain temps, pendant l'exécution des instructions suivantes du programme secondaire et du programme principal.

Un schéma-bloc d'un composant électronique correspondant à ce deuxième mode de réalisation de l'invention est représenté sur la figure 2.

En plus des éléments déjà décrits qui portent les mêmes références que sur la figure 1, le composant électronique comprend une pompe de charges 9.

Cette pompe de charges est normalement prévue pour fournir une haute tension V_{PP} de programmation et/ou d'effacement à partir de la tension d'alimentation V_{CC} pour permettre la programmation et/ou l'effacement de données dans une mémoire non volatile programmable et/ou effaçable électriquement, comme par exemple les mémoires communément appelées mémoires EPROM, EEPROM ou encore flash EPROM. Dans l'invention, cette pompe de charges est associée à la mémoire programme.

Dans l'exemple, elle est activée par un signal d'écriture WE de la mémoire programme.

Une telle pompe a comme caractéristique connue de consommer beaucoup de courant pendant le temps d'établissement de la haute tension en sortie et le

temps de la programmation ou de l'effacement, ce qui peut être de l'ordre de quelques millisecondes. En activant une telle pompe, par exemple, en prévoyant une instruction de programmation dans le programme
5 secondaire, on surimpose donc une forte consommation en courant qui va masquer la consommation des instructions suivantes du programme secondaire et du programme principal.

L'invention ne se limite pas aux modes de
10 réalisation ou aux variantes décrits. Elle couvre toute utilisation de moyens pour suspendre le programme principal à des moments aléatoires pendant un temps qui peut-être fixe, variable ou aléatoire, avec ou sans l'utilisation de moyens pour ajouter une consommation
15 en courant supplémentaire.

Avec un tel masquage ou brouillage en utilisant l'une quelconque des variantes de l'invention ou une combinaison de celles-ci, aucun traitement statistique ne devient possible.

20 En pratique, le choix de tel ou tel programme secondaire peut dépendre de l'application à laquelle le composant électronique est destiné.

L'invention s'applique à tous les composants comprenant au moins un compteur et un générateur
25 aléatoire. Pour un composant électronique donné, le choix de tel ou tel programme secondaire dépend des ressources du composant considéré, de l'efficacité en rapport avec l'application considérée.

On peut aussi prévoir d'utiliser différents
30 programmes secondaires, ce qui permet de mélanger les genres, pour améliorer le brouillage, le choix du programme secondaire à exécuter se faisant alors en début de routine d'interruption.

Un tel composant est tout particulièrement
35 utilisable dans les cartes à puces, pour améliorer leur inviolabilité.

REVENDEICATIONS

1. Composant électronique comprenant au moins un microprocesseur (1) et des moyens de mémorisation (2, 3) pour exécuter un programme principal, caractérisé en ce qu'il comprend en outre un compteur (4) d'une valeur aléatoire (R), ledit compteur générant en sortie un signal d'information de fin de comptage (IT0) pour suspendre l'exécution dudit programme principal le temps de l'exécution d'un programme secondaire par le microprocesseur.

2. Composant électronique selon la revendication 1, caractérisé en ce que le temps d'exécution du programme secondaire est constant.

3. Composant électronique selon la revendication 1, caractérisé en ce que le temps d'exécution du programme secondaire est variable.

4. Composant électronique selon la revendication 3, caractérisé en ce que le temps d'exécution du programme secondaire est aléatoire.

5. Composant électronique selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre des moyens consommateur de courant activés par le programme secondaire.

6. Composant électronique selon la revendication 5, caractérisé en ce que ces moyens consommateur de courant comprennent une pompe de charges (9).

7. Composant électronique selon la revendication 5 ou 6, caractérisé en ce que ces moyens comprennent des instructions entraînant une consommation instantanée.

8. Procédé pour masquer l'exécution d'opérations ou la manipulation de données dans un composant électronique (CI) comprenant un microprocesseur (1) et des moyens de mémorisation (2, 3) pour exécuter un programme principal, caractérisé en ce que ce procédé consiste à utiliser un générateur (5) d'une valeur aléatoire (R) et un compteur (4) pour suspendre l'exécution du programme principal à des instants aléatoires, le temps de l'exécution d'un programme secondaire.

9. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur (4) avec cette nouvelle valeur et à autoriser le décomptage avant de retourner à l'exécution du programme principal.

10. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire est exécutable en temps aléatoire.

11. Procédé selon la revendication 10, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à décompter jusqu'à zéro cette nouvelle valeur aléatoire dans une boucle du programme secondaire, puis à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur à cette nouvelle valeur et à

activer le compteur avant de retourner à l'exécution du programme principal.

12. Procédé selon l'une quelconque des revendications 8 à 11, caractérisé en ce que le programme secondaire active en outre des moyens de consommation de courant.

13. Procédé selon la revendication 12, caractérisé en ce que les dits moyens de consommation de courant comprennent une pompe de charges (9).

14. Procédé selon la revendication 12 ou 13, caractérisé en ce que ces moyens comprennent des instructions provoquant une consommation en courant instantanée.

15. Procédé selon l'une quelconque des revendications 8 à 14, caractérisé en ce qu'il comprend différents programmes secondaires.



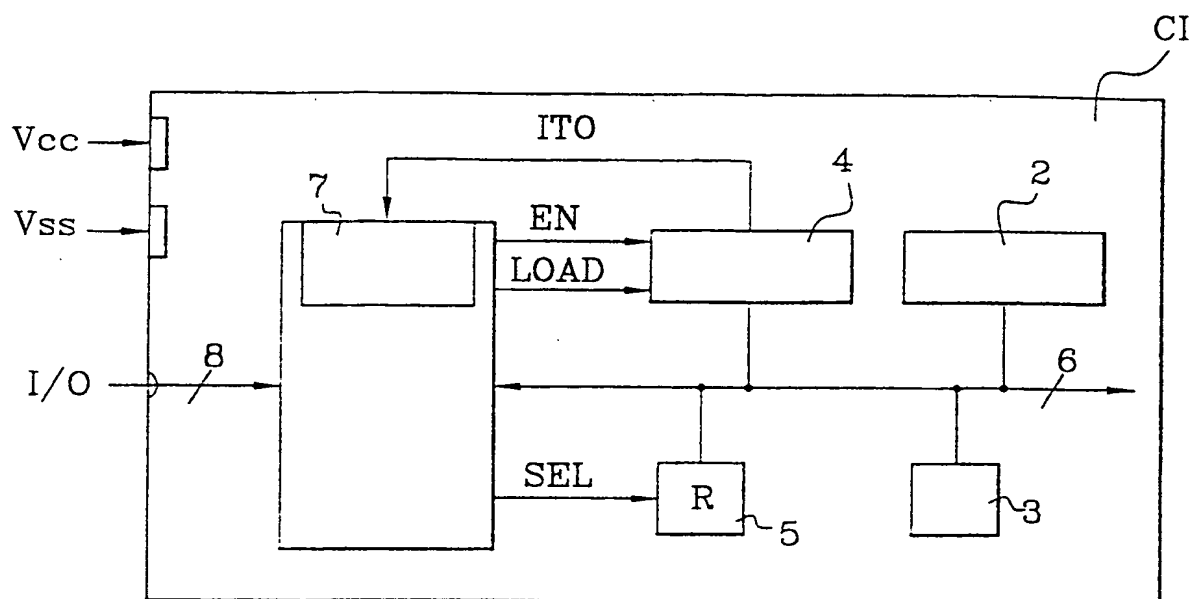
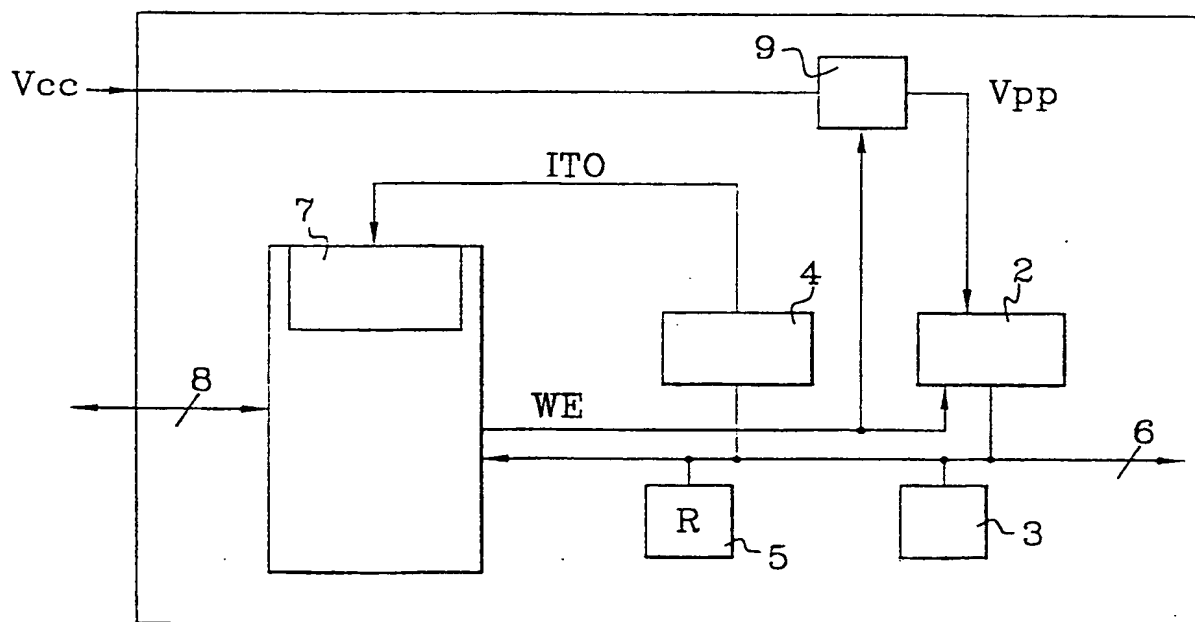
5

5

5

5

1/1

FIG.1FIG.2



1

2

3

4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/02521

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 September 1997 (1997-09-12) page 6, line 1 -page 12, line 12; figures 1,8	1-15
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 September 1991 (1991-09-25)	1,3-5,8, 10-12,15
A	column 3, line 25 -column 4, line 53; figures 1,2	2,6,7,9, 13,14
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) abstract	1,6,9,13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

12 January 2000

Date of mailing of the international search report

20/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Moens, R

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/02521

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9733217 A	12-09-1997	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998

RAPPORT DE RECHERCHE INTERNATIONALE

De l'Union internationale No

PCT/FR 99/02521

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement):

CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 33217 A (UGON MICHEL ; BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) page 6, ligne 1 - page 12, ligne 12; figures 1,8	1-15
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25)	1,3-5,8, 10-12,15
A	colonne 3, ligne 25 - colonne 4, ligne 53; figures 1,2	2,6,7,9, 13,14
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 juin 1990 (1990-06-05) abrégé	1,6,9,13

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

12 janvier 2000

Date d'expédition du présent rapport de recherche internationale

20/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Moens, R

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Date Internationale No

PCT/FR 99/02521

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9733217 A	12-09-1997	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998

PCT

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT

(règle 92bis.1 et
instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

NONNENMACHER, Bernard
Gemplus
Parc d'Activités de Gémenos
Avenue du Pic de Bertagne
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année) 03 octobre 2000 (03.10.00)	
Référence du dossier du déposant ou du mandataire GEM 585	NOTIFICATION IMPORTANTE
Demande internationale no PCT/FR99/02521	Date du dépôt international (jour/mois/année) 15 octobre 1999 (15.10.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse GEMPLUS S.C.A. Parc d'Activités de Gémenos Avenue du Pic de Bertagne F-13881 Gémenos Cedex FRANCE	Nationalité (nom de l'Etat) FR	Domicile (nom de l'Etat) FR
	no de téléphone	
	no de télécopieur	
	no de téléimprimeur	

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☒ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse GEMPLUS Parc d'Activités de Gémenos Avenue du Pic de Bertagne F-13881 Gémenos Cedex FRANCE	Nationalité (nom de l'Etat) FR	Domicile (nom de l'Etat) FR
	no de téléphone	
	no de télécopieur	
	no de téléimprimeur	

3. Observations complémentaires, le cas échéant:

La correction du nom s'applique également à l'adresse du mandataire.

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur ☐ aux offices désignés concernés
☐ à l'administration chargée de la recherche internationale ☒ aux offices élus concernés
☒ à l'administration chargée de l'examen préliminaire international ☐ autre destinataire:

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur (41-22) 740.14.35	Fonctionnaire autorisé: Ellen Moyse no de téléphone (41-22) 338.83.38
---	---

This Page Blank (uspto)

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 09 juin 2000 (09.06.00)	
Demande internationale no PCT/FR99/02521	Référence du dossier du déposant ou du mandataire GEM 585
Date du dépôt international (jour/mois/année) 15 octobre 1999 (15.10.99)	Date de priorité (jour/mois/année) 16 octobre 1998 (16.10.98)
Déposant ANGUITA, Philippe etc	

1. L'office désigné est avisé de son élection qui a été faite:

☒

dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

15 mai 2000 (15.05.00)

☐

dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection

☒

a été faite

☐

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé Diana Nissen no de téléphone: (41-22) 338.83.38
--	--

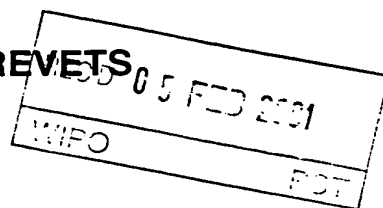
This Page Blank (uspto)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)





Référence du dossier du déposant ou du mandataire GEM 585	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02521	Date du dépôt international (jour/mois/année) 15/10/1999	Date de priorité (jour/mois/année) 16/10/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F1/00		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.
 - ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 3 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:
 - I ☒ Base du rapport
 - II ☐ Priorité
 - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
 - IV ☐ Absence d'unité de l'invention
 - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
 - VI ☐ Certains documents cités
 - VII ☒ Irrégularités dans la demande internationale
 - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 15/05/2000	Date d'achèvement du présent rapport 01.02.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Quesson, C N° de téléphone +49 89 2399 2667 

This Page Blank (uspto)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02521

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17.)*) :

Description, pages:

1-8 version initiale

Revendications, N°:

1-15 reçue(s) le 21/10/2000 avec la lettre du 19/10/2000

Dessins, feuilles:

1 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

This Page Blank (uspto)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02521

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-15
	Non : Revendications
Activité inventive	Oui : Revendications 1-15
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-15
	Non : Revendications

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

This Page Blank (uspto)

Concernant le point V Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence au/x/ document/s/ suivant/s/:

D1: WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997
(1997-09-12)

D2: EP-A-0 448 262 (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25)

D3: US-A-4 932 053 (FRUHAUF SERGE ET AL) 5 juin 1990 (1990-06-05)

1.1. Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet des revendications 1-15, se place dans le même contexte technique (pages 1 et 2) et décrit (voir en particulier les passages cités dans le rapport de recherche) un circuit intégré et le procédé d'utilisation d'un tel circuit intégré, qui possède des moyens tant de décorrélation du déroulement d'au moins une d'instruction d'un programme avec les signaux électriques internes ou externes du circuit intégré. En particulier, les moyens de décorrélation comprennent un système chargeant une valeur aléatoire dans un registre commandant les bits de masquage d'interruption du processeur. Les séquences secondaires sont choisies aléatoirement et de durées pouvant être variables - éventuellement aléatoirement - (p. 3, l. 17-23).

1.2. D2 vise aussi le même contexte technique que la demande, et propose (voir en particulier les passages cités dans le rapport de recherche) d'éviter la détermination du moment d'exécution d'une routine par rapport à un événement observable de l'extérieur, en faisant varier aléatoirement la durée entre ledit événement et l'exécution d'une routine donnée, en faisant exécuter avant cette routine donnée une ou plusieurs routines secondaires (INTERIM ROUTINE 1 à M) dont les paramètres, la durée et la combinaison peuvent être changés de façon aléatoire.

1.3. D3 décrit un dispositif de sécurité contre la détection non autorisée de données protégées, en particulier par l'observation de la consommation de courant d'un circuit intégré. Le dispositif active la simulation, suivant une séquence pseudo aléatoire, de consommations de valeurs identiques à celles de cellules mémoires réelles.

This Page Blank (uspto)

2. D1 et D2 proposent différentes variations concernant la durée de la ou des routines secondaires - l'ensemble des routines de D2 pouvant être considérées, le cas échéant, comme une routine secondaire unique de durée variable ou *aléatoire* -.

Par contre, l'aspect *aléatoire* de la gestion des interruptions selon D1 se limite à ce que le processeur (Fig. 1) peut charger une valeur aléatoire, fournie par le générateur aléatoire 2, dans le registre R1 de masquage des interruptions.

D1 ne divulgue donc pas l'une des caractéristiques des revendications 1 et 8 telles que clarifiées, à savoir l'utilisation d'un compteur apte à interrompre par un signal de fin de comptage d'une valeur aléatoire provenant d'un générateur aléatoire interne le programme principal pour lui faire exécuter le programme secondaire, le compteur constituant ainsi une nouvelle source d'interruption.

D2, selon lequel le branchement vers la ou les routines intermédiaires ou secondaires se fait toujours au même point de la routine principale (à savoir après la sous-routine N-1 et avant la routine N), plutôt qu'à un instant aléatoire, par interruption, ne divulgue ni ne suggère pas non plus ces caractéristiques revendiquées.

Les revendications 1-15 satisfont donc aux exigences de l'article 33(1) PCT.

Pour mémoire, il est noté que l'inclusion dans le composant de moyens spécifiques destinés à provoquer - à partir de leur déclenchement par le programme secondaire - une forte consommation de courant masquant celle des instructions suivantes des programmes secondaire et primaire (revendications 6 et 13, page 7, lignes 10-16), n'est pas divulguée ni même suggérée dans les documents disponibles de l'art antérieur.

Concernant le point VII Irrégularités dans la demande internationale

1. Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le/les/ document/s/ D1, D2 et D3 et ne cite pas ce/ces document/s/.

2. La description aurait dû être adaptée pour concorder avec les revendications modifiées, comme l'exige la règle 5.1 a) iii) PCT.

This Page Blank (uspto)

REVENDEICATIONS

1. Composant électronique comprenant au moins un microprocesseur (1), des moyens de mémorisation (2, 3) pour exécuter un programme principal et un générateur
5 (5) d'une valeur aléatoire, caractérisé en ce qu'il comprend en outre un compteur (4) d'une valeur aléatoire (R), ledit compteur générant en sortie un signal d'information de fin de comptage appliqué comme
signal d'interruption du microprocesseur (IT0) pour
10 suspendre l'exécution dudit programme principal le temps de l'exécution d'un programme secondaire par le microprocesseur.

2. Composant électronique selon la revendication 1,
15 caractérisé en ce que le temps d'exécution du programme secondaire est constant.

3. Composant électronique selon la revendication 1, caractérisé en ce que le temps d'exécution du programme
20 secondaire est variable.

4. Composant électronique selon la revendication 3, caractérisé en ce que le temps d'exécution du programme
secondaire est aléatoire.

25

5. Composant électronique selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre des moyens consommateur de courant
activés par le programme secondaire.

30

6. Composant électronique selon la revendication 5, caractérisé en ce que ces moyens consommateur de courant comprennent une pompe de charges (9).

This Page Blank (uspto)

7. Composant électronique selon la revendication 5 ou 6, caractérisé en ce que ces moyens comprennent des instructions entraînant une consommation instantanée.

5 8. Procédé pour masquer l'exécution d'opérations ou la manipulation de données dans un composant électronique (CI) comprenant un microprocesseur (1), des moyens de mémorisation (2, 3) pour exécuter un programme principal et un générateur (5) d'une valeur
10 aléatoire (R), caractérisé en ce que ce procédé consiste à utiliser un compteur (4) générant en sortie un signal de fin de comptage d'une valeur aléatoire fournie par ledit générateur, appliqué comme signal d'interruption du microprocesseur pour suspendre
15 l'exécution du programme principal à des instants aléatoires, le temps de l'exécution d'un programme secondaire.

20 9. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur (4) avec cette nouvelle valeur et à autoriser le décomptage avant de retourner à l'exécution du programme principal.

25

10. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire est exécutable en temps aléatoire.

30 11. Procédé selon la revendication 10, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à décompter jusqu'à zéro cette nouvelle valeur aléatoire dans une boucle du programme secondaire, puis

This Page Blank (uspto)

à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur à cette nouvelle valeur et à activer le compteur avant de retourner à l'exécution du programme principal.

5

12. Procédé selon l'une quelconque des revendications 8 à 11, caractérisé en ce que le programme secondaire active en outre des moyens de consommation de courant.

10

13. Procédé selon la revendication 12, caractérisé en ce que les dits moyens de consommation de courant comprennent une pompe de charges (9).

15

14. Procédé selon la revendication 12 ou 13, caractérisé en ce que ces moyens comprennent des instructions provoquant une consommation en courant instantanée.

20

15. Procédé selon l'une quelconque des revendications 8 à 14, caractérisé en ce qu'il comprend différents programmes secondaires.

This Page Blank (uspto)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

6

09/807614
Translation
0500

Applicant's or agent's file reference GEM 585		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR99/02521	International filing date (day/month/year) 15 October 1999 (15.10.99)	Priority date (day/month/year) 16 October 1998 (16.10.98)	
International Patent Classification (IPC) or national classification and IPC G06F 1/00		RECEIVED AUG 31 2001	
Applicant GEMPLUS		Technology Center 2100	

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability: citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 15 May 2000 (15.05.00)	Date of completion of this report 01 February 2001 (01.02.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/02521

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 1-4 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

☐ the international application as originally filed.

☒ the description. pages 1-8 . as originally filed.

pages _____ . filed with the demand.

pages _____ . filed with the letter of _____ .

pages _____ . filed with the letter of _____ .

☒ the claims. Nos. _____ . as originally filed.

Nos. _____ . as amended under Article 19.

Nos. _____ . filed with the demand.

Nos. 1-15 . filed with the letter of 19 October 2000 (19.10.2000) .

Nos. _____ . filed with the letter of _____ .

☒ the drawings. sheets/fig 1 . as originally filed.

sheets/fig _____ . filed with the demand.

sheets/fig _____ . filed with the letter of _____ .

sheets/fig _____ . filed with the letter of _____ .

2. The amendments have resulted in the cancellation of:

☐ the description. pages _____

☐ the claims. Nos. _____

☐ the drawings. sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/02521

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-15	YES
	Claims		NO
Inventive step (IS)	Claims	1-15	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-15	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following document/s/:

D1: WO 97 33217 A (UGON MICHEL; BULL CP8 (FR)
12 September 1997 (1997-09-12)
D2: EP-A-0 448 262 (GEN INSTRUMENT CORP)
25 September 1991 (1991-09-25)
D3: US-A-4 932 053 (FRUHAUF SERGE ET AL)
5 June 1990 (1990-06-05)

1.1. Document D1, which is considered to be the closest prior art to the subject matter of Claims 1 to 15, belongs to the same technical context (pages 1 and 2). It describes (in particular see the passages cited in the search report) an integrated circuit, and the method for using such an integrated circuit, which has means for decorrelating at least one programme instruction sequence from the internal or external electrical signals of the integrated circuit. In particular, the decorrelation means comprise a system which loads a random value into a register controlling the processor interrupt masking bits. The secondary sequences are chosen at random and the durations thereof can be varied, possibly randomly - (p. 3, lines 17 to 23).

this Page Blank (uspto)

1.2 D2 relates to the same technical context as the application, and suggests (in particular see the passages cited in the search report) preventing determination of the time of execution of a routine in relation to occurrence of an observable external event by randomly varying the duration between said event and the execution of a given routine by executing one or more secondary routines (INTERIM ROUTINE 1 to M), whose parameters, duration and combination can be randomly changed, before this routine.

1.3 D3 describes a safety device against the unauthorised detection of protected data, specifically by observing the current consumption of an integrated circuit. The device actuates the simulation, according to a pseudo-random sequence of consumption values identical to those of real memory cells.

2. D1 and D2 suggest different variations concerning the duration of the secondary routine(s) (the entire set of routines of D2 may, when appropriate, be considered as a single secondary routine of variable, or *random*, duration).

The *random* aspect of managing interruptions as per D1, however, consists only in that the processor (Figure 1) can load a random value provided by the random number generator 2 into the interrupt masking register R1. Therefore D1 does not disclose one of the features of Claims 1 and 8 as clarified, that is, the use of a counter which is able, by using a random value end-of-counting signal from an internal random number generator, to interrupt the main programme in order to make it execute a secondary programme. The counter thus constitutes a new source of interruption.

This Page Blank (uspto)

D2, according to which the branch to the interim or secondary routine(s) is always taken at the same point in the main routine (that is after the sub-routine N-1 and before the routine N) rather than at a random moment, by interruption, does not disclose or suggest these claimed features.

Claims 1 to 15 therefore also satisfy the requirements of PCT Article 33(1).

It should be noted that the inclusion in the component of specific means for causing a high consumption of current, activated by the secondary programme, masking consumption by the subsequent instructions of the secondary and primary programmes (Claims 6 and 13, page 7, lines 10 to 16), is not disclosed nor even suggested in the available prior art.

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/02521

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not indicate the relevant prior art set out in document/s/ D1, D2 and D3 and does not cite that/those/ document/s.
2. The description should have been changed in order to bring it in line with the modified claims, as per PCT Rule 5.1(a)(iii).

This Page Blank (uspto)